JOHN M. NEUKOM (SBN 275887)
DEBEVOISE & PLIMPTON, LLP
650 California Street
San Francisco, CA 94108
Telephone: (415) 738-5700
Facsimile: (415) 644-5628
jneukom@debevoise.com

JAMES Y. PAK (SBN 304563)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
525 University Avenue
Palo Alto, California 94301-1908
Telephone: (650) 470-4500
Facsimile: (650) 470-4570
james.pak@skadden.com

DOUGLAS R. NEMEC (*pro hac vice*)
LESLIE A. DEMERS (*pro hac vice*)
ANTHONY P. BIONDO (*pro hac vice*)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
One Manhattan West
New York, New York 10001
Telephone: (212) 735-3000
Facsimile: (212) 735-2000
douglas.nemec@skadden.com
leslie.demers@skadden.com
anthony.biondo@skadden.com

Attorneys for Plaintiff,
FORTINET, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FORTINET, INC.,

Plaintiff,

v.

FORESCOUT TECHNOLOGIES, INC.,

Defendant.

Case No. 3:20-cv-03343-EMC

PLAINTIFF FORTINET, INC.'S OPENING CLAIM CONSTRUCTION BRIEF

Hon. Edward M. Chen

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

I. INTRODUCTION

The Asserted Patents relate to network access control. Plaintiff Fortinet has asserted five patents, U.S. Patents No. 9,369,299; 8,458,314; 9,948,662; 9,894,034; and 9,503,421 (the "Fortinet Patents"), and Defendant Forescout has asserted six patents, U.S. Patents No. 6,363,489; 8,590,004; 9,027,079; 10,530,764; 10,652,116 and 10,652,278 (the "Forescout Patents") (collectively, the "Asserted Patents"). Given the number of patents at issue, the parties and the Court have agreed to limit the briefing to eight terms per side, although neither party waives the right to seek resolution of the other issues identified in the Joint Claim Construction and Prehearing Statement. This opening brief from Fortinet addresses the eight terms that Fortinet believes are most critical to resolving this case, relating to each of Forescout's Asserted Patents.

While the six Forescout Patents come from five patent families, they all suffer similar defects that render them indefinite. These defects fall broadly into two categories: (i) they recite terms that fail to provide clear notice to the public of the boundaries of the claimed subject matter, and (ii) they recite "function without reciting sufficient structure for performing that function," and disclose no corresponding structure or algorithm in the specification. *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1349 (Fed. Cir. 2015) (en banc). In the former category, two of Defendant's patents recite that various components are "dynamic" without explaining how these components would vary from their non-dynamic counterparts; one recites that a device is a "corporate" device without providing any guidance on how to discern a corporate device from a non-corporate device; and another recites that certain rules must be "standard based" without explaining what is or is not a "standard" and what it means for a rule to be "based" upon one. In the latter category, three of Defendant's patents recite bare function and/or a "module" to perform this bare function, without disclosing any corresponding algorithm or structure. Such claims are indefinite.

Rather than proposing alternative constructions for these terms or attempting compromise, Defendant submitted that no terms in its six patents require construction, and that all of Fortinet's identified eight terms should be afforded their plain and ordinary meaning. As described below, however, the scope of these terms is far from clear to an ordinarily skilled artisan.

II. THE ASSERTED PATENTS

The six patents asserted by Defendant relate to network access control or network security in general and come from five patent families. The '489 Patent relates to intrusion detection by provisioning and sending "specially crafted" "earmarks" after detecting an information gathering procedure. The '004 and '079 Patents relate to the enforcement of "dynamic security policy." The '116 Patent relates to the use of data from two sources to determine a "device type classification" of devices on a network. The '278 Patent relates to monitoring devices on a network by using "standard based" compliance rules. Finally, the '764 Patent relates to validating "corporate" devices by checking certificates after they connect to a network. Each one attempts to broadly claim an idea for a method and/or a system, sacrificing clarity of scope in favor of the potential for increased breadth. Some of these patents reference generic "modules" for carrying out functions, or recite the same bare functions in method versions of the claims without describing structure, and failing to "disclose an algorithm for performing the claimed function." *Net MoneyIN, Inc. v. VeriSign, Inc.*, 545 F.3d 1359, 1367 (Fed. Cir. 2008). Others introduce words into the claims – like "dynamic," "corporate," or "standard based" – that, in context, do not serve to "inform those skilled in the art about the scope of the invention with reasonable certainty." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014).

III. LEGAL STANDARDS

The purpose of claim construction is to "define the scope of the patented invention and the patentee's right to exclude." *HTC Corp. v. Cellular Commc'ns Equip., LLC*, 877 F.3d 1361, 1367 (Fed. Cir. 2017). It is a question of law to be decided by the Court, although it may have factual underpinnings. *Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1357 (Fed. Cir. 2016). The words of a claim are generally given their "ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312-13 (Fed. Cir. 2005). The inquiry into how a person of ordinary skill in the art interprets a claim term "provides an objective baseline from which to begin claim interpretation." *Id.* at 1313. At times, a patentee may use claim language idiosyncratically, necessitating a look into "those sources available to the public that show what a person of skill in the art would have understood disputed claim language to mean."

Id. at 1314. A person of ordinary skill reads the claim term "not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id*. at 1313. Thus, a Court reviews intrinsic evidence, such as "the words of the claims themselves, the remainder of the specification, the prosecution history," and extrinsic evidence "concerning relevant scientific principles, the meaning of technical terms, and the state of the art." *Id.* at 1314.

1. Indefiniteness - § 112(b) / § 112 ¶ 2

A patent must include "claims particularly pointing out and distinctly claiming the subject matter which the inventor … regards as the invention." 35 U.S.C. § 112(b). A claim is indefinite when, "read in light of the patent's specification and prosecution history, [it] fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus*, 572 U.S. at 898-99. Indefiniteness is "a legal determination arising out of the court's performance of its duty construing the claims." *BJ Servs. Co. v. Halliburton Energy Servs., Inc.*, 338 F.3d 1368, 1372 (Fed. Cir. 2003). Though factual issues may underlie this legal determination, "a court has some discretion in deciding whether to address indefiniteness at the claim construction phase." *Dali Wireless, Inc. v. Corning Optical Commc'ns LLC*, No. 20-cv-06469-EMC, 2021 WL 3037700, at *16 (N.D. Cal. July 19, 2021) (Chen, J.). In any event, the "factual underpinnings involved in claim construction are similar to the factual underpinnings involved in indefiniteness inquiries." *Id.* The test for indefiniteness "mandates clarity, while recognizing that absolute precision is unattainable." *Nautilus*, 572 U.S. at 899. Overall, "it cannot be sufficient that a court can ascribe some meaning to a patent's claim; the definiteness inquiry trains on the understanding of a skilled artisan at the time of the patent application, not that of a court viewing matters post hoc." *Id.* at 911. If an accused infringer shows by clear and convincing evidence that a claim fails to meet this "reasonable certainty" standard, the claim is invalid. *Id.* at 910.

2. Functional Claiming - § 112(f) / § 112 ¶ 6

A patent claim is expressed in means-plus-function form when it recites "means or step[s] for performing a specified function without the recital of structure, material, or acts in support thereof." 35 U.S.C. § 112(f). Such means-plus-function claims must "be construed to cover the corresponding

structure, material, or acts described in the specification and equivalents thereof." *Id.* When a patent invokes this rule "by reciting a function to be performed rather than by reciting structure for performing that function," constraints apply to "[restrict] the scope of coverage to only the structure, materials, or acts described in the specification as corresponding to the claimed function and equivalents thereof." *Williamson*, 792 F.3d at 1347. If the claim is not explicitly drafted using the word "means," the proponent of such a construction must show that these rules nonetheless apply by showing that claim otherwise fails to recite sufficiently definite structure. *Id.* at 1350. If the means-plus-function rules apply, the Court engages in a two-step inquiry to construe the claim where it first "identif[ies] the claimed function," and then "determine[s] what structure, if any, disclosed in the specification corresponds to the claimed function." *Id.* at 1351. Moreover, if there are multiple claimed functions, the patent "must disclose adequate corresponding structure to perform *all* of the claimed functions." *Id.* at 1351-32 (emphasis added). In the case of computer-implemented inventions, "structure" refers to "algorithmic structure for implementing the claimed functions." *Id.* at 1350. If the specification "fails to disclose adequate corresponding structure, the claim is indefinite" and the claim is thus invalid. *Id.* at 1352.

IV. CLAIM CONSTRUCTION

1. U.S. Patent No. 6,363,489

a. "earmark provisioning module" and "returning an earmark"

Fortinet's Proposed Construction	Defendant's Proposed Construction
Indefinite	Plain and Ordinary Meaning

Claims 1 and 15 of the '489 Patent recite, respectively, a method and system for detecting and handling a communication from an unauthorized source on the network. The claims are based upon a method of seeding "earmarks" with false information to suspected intruders and looking for those earmarks in later communications. Claim 15 recites:

> 15. A system for detecting and handling the communication from an unauthorized source on a network, the system comprising:
>
> (a) An entry point to the network such that the communication passes through said entry point to reach the network;
>
> *(b) An **earmark provisioning module** for preparing earmarks for sending to unauthorized source, such that said earmarks are specially crafted false data that will identify an unauthorized source;*

> (c) An intrusion detection module for analyzing the communication and for detecting said earmark in the communication; and
>
> (d) An intrusion-handling module for handling the communication if said earmark is detected by said intrusion detection module.

And, Claim 1 recites:

> 1. A method for detecting and handling a communication from an unauthorized source on a network, the method comprising the steps of:
>
> (a) receiving the communication from the unauthorized source;
>
> (b) analyzing the communication for detecting an information gathering procedure;
>
> (c) if said information-gathering procedure is detected, indicating a source address of the communication as a suspected network reconnaissance collector;
>
> *(d)* ***returning an earmark*** *to said suspected reconnaissance collector, such that said earmark includes specially crafted false data, and such that said earmark includes data that can serve to identify an unauthorized source;*
>
> (e) analyzing each subsequent communication for a presence of said earmark;
>
> (f) if said earmark is present, indicating source address of the communication as a suspected network reconnaissance collector, and
>
> (g) if said source address is said intruder source address, applying intrusion handling procedures towards the communication from said intruder source address.

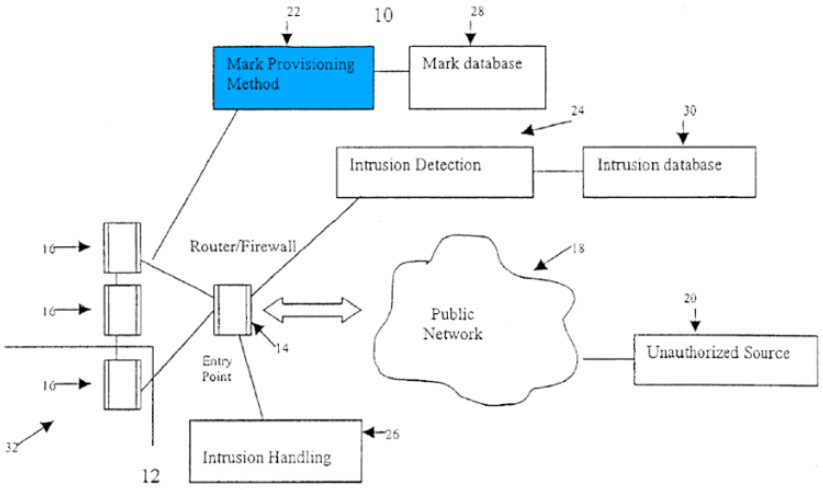
As shown above, Claim 15, the system claim, recites an "earmark provisioning module" which provisions these earmarks. Claim 1, the method claim, recites the step of "returning an earmark." Both claims provide that these earmarks include "specially crafted false data" such that they can "identify an unauthorized source," but neither recites *how* these earmarks are "specially crafted," and neither recites how these earmarks serve to "identify" a source. Thus, these earmarks are described entirely by their function, identifying a source, with the claims' only reference to structure being the fact that they are "specially crafted," a term that provides a POSITA with no guidance other than that they must be "special" in some way. *See, e.g., Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014) (noting that "highly subjective" terms provide little guidance to one of skill in the art and can render a claim indefinite). Shamos Decl. (Ex. A) ¶ 38.

Despite not using the words "means for" or "step for," these purely functional recitations invoke § 112 ¶ 6 because they recite "function without reciting sufficient structure for performing that function" when it comes to the provisioning of the "earmarks" crucial to understanding the claim.

Williamson, 792 F.3d at 1348-50. With computer-implemented claims, structure refers to "algorithmic structure for implementing the claimed functions." *Id.* at 1350. Here, the system claim explicitly uses the word "module," which is a "well-known nonce word that can operate as a substitute for 'means.'" *Id.*; *see also, e.g., Rain Computing, Inc. v. Samsung Elecs. Am., Inc.*, 989 F.3d 1002, 1006 (Fed. Cir.) (holding a "user identification module" to invoke § 112 ¶ 6 and finding the claim indefinite), *cert. denied*, 142 S. Ct. 579 (2021). It then recites the function performed by this module – "preparing earmarks" by "specially craft[ing]" false data to identify intruders – without explaining how, algorithmically, this "special" crafting works, or what this false data comprises, and what is false about it. The corresponding method claim recites an identical function without reference to the component producing the earmarks. In short, the "earmark provisioning module" is a "term coined for the purposes of the patents-in-suit," that refers to the generation of an "earmark," itself a coined term. *Advanced Ground Info. Sys., Inc. v. Life360, Inc.*, 830 F.3d 1341, 1348 (Fed. Cir. 2016) (holding a "symbol generator" to invoke § 112 ¶ 6 and finding the claim indefinite); Shamos Decl. ¶ 31. Moreover, even the earmarks produced by this "module" are defined entirely by their function: they must "identify" an intruder, but how this is done is left out in favor of a "high level" recitation that fails to "inform the structural character" of the earmark provisioning process. *Williamson*, 792 F.3d at 1351.

The specification does not "disclose an algorithm for performing the claimed function," and thus the claims are indefinite. *Advanced Ground Info. Sys.*, 830 F.3d at 1349; Shamos Decl. ¶ 41. The terms "earmark," "earmark provisioning," and "earmark provisioning module" are not terms of art, and do not even appear in the specification of the patent. Shamos Decl. ¶ 31. The specification refers to "marks" in several places, and given that these serve the same function, this suggests that the "earmark" of the claims may be a type of "mark." However, even charitably assuming they refer to the same thing (despite the use of different terms), the specification provides vanishingly little guidance on what a "mark" actually is, and how it is "crafted." The disclosure refers to the same functionality described in the claim, along with some examples of types of false data that one might include in a mark, although it includes no examples of actual earmarks in their entirety. *See* '489 Patent at 4:61-5:14; Shamos Decl. ¶ 41. It describes that this module "provides this information,"

presumably the mark, "according to techniques which matches the probing method used by unauthorized users to gather information," without explaining what those techniques are. '489 Patent at 5:4-6. When the specification does refer to the provisioning of this "mark," it does so with a block containing the "mark provisioning method," a term which does not appear in the specification except for a single black box in a figure, attached to a "mark database," an unclaimed element for storing these marks:



'489 Patent at FIG. 1 (emphasis added)

In *Advanced Ground Information Systems*, the Federal Circuit found indefinite a similar term, "signal generator," when the specification described "in general terms" that a signal was generated "based on" certain information, but did not disclose an algorithm. 830 F.3d at 1349. There, the court rejected the argument that the specification described the potential use of a database in the symbol generation process, much like the "mark database" of FIG. 1 in the '489 Patent, as it "only address[ed] the medium through which the symbols are generated," and not the actual means of generation. *Id.* The court reiterated that the patent must "disclose an algorithm for performing the claimed function," and held the patent invalid, as a failure to do so "amounts to pure functional claiming." *Id.* Here too, the actual algorithm for generating the "earmarks" crucial to the asserted claims of the '489 Patent is absent, rendering it indefinite.

Defendant's expert, Dr. Cole, describes his belief that these terms need no construction. Cole Decl. (Ex. B) ¶ 28-34. And yet, he also then advances theories as to what is "special" about the crafting of the data. He argues that the data must be "specially crafted to present an appealing target," as

opposed to being "other false data" such as that "generated randomly without any purpose." *Id.* ¶ 32. That Defendant's own expert reads the specification to require that this data be generated with a specific "purpose" proves that the patent provides no objective guidance, or is "at best muddled," when describing the "highly subjective" requirement that the earmark provisioning step create data that is in some way "specially crafted." *Interval Licensing*, 766 F.3d at 1371-72. Even to the extent the patent provides limited examples of false data, it does not explain what about the data is false, how the data is "specially crafted," or anything about the earmark provisioning process. In fact, during prosecution, the Examiner rejected an attempted amendment to the claim to specify that this earmark must further "remain[] concealed from the unauthorized source," as not being enabled by the patent, demonstrating just how bare the disclosure is as it pertains to these earmarks. Ex. C, Final Rejection dated Aug. 28, 2001, at 2; Shamos Rep ¶ 40. Even if the claim term is not read as invoking § 112 ¶ 6, the "special crafting" of these earmarks is so vague as to independently render the claim indefinite, and certainly lacks the connotation of structure necessary to avoid such an invocation, and to avoid indefiniteness both in the claim and the specification.

2. U.S. Patent Nos. 8,590,004 and 9,027,079

a. "dynamic security policy" (Both)

Fortinet's Proposed Construction	Defendant's Proposed Construction
Indefinite	Plain and Ordinary Meaning

Claim 10 in both the '004 and '079 Patents recites that certain data is processed according to a "dynamic security policy." Both related patents use this term in substantially the same way. The '004 Patent recites, in relevant part, a method including the step of:

> … processing the retrieved data from the authentication server and the DSDPD, wherein said processing is computed according to a **dynamic security policy**; …

And, the '079 Patent recites, in relevant part, a method including the step of:

> … performing a first processing of the retrieved data from the authentication server and the DSDPD, wherein said first processing is computed according to a **dynamic security policy**; …

Additionally, each patent recites a "Dynamic Security Data & Policy Database" in this and other claims, which would also involve a "Dynamic Security … Policy," although this term is discussed separately below. In any event, the issue with this term arises from the phrase "dynamic," which does

not "inform those skilled in the art about the scope of the invention with reasonable certainty" because it does not explain what is dynamic about the policy. *Nautilus*, 572 U.S. at 910.

The phrase "dynamic" can have many interpretations – it could mean that the policy is subject to change, or that it changes in response to specific events, or that it is triggered by a series of events. Shamos Decl. ¶ 56. Nothing in the intrinsic evidence resolves this ambiguity, and the specifications use the word "dynamic" only when stating the full name of the DSDPD, the "dynamic security data and policy database," the related DSASP, or "dynamic security authentication and proxy server," and when using the phrase "dynamic security policy" itself, apart from the title. Shamos Decl. ¶ 57; '004 Patent at 1:1, 1:10, 2:21, 2:36-37, 2:40, 6:7, 6:23, 6:27, 8:51, 8:54, 9:13, 9:56, 11:2; '079 Patent, at 1:1, 1:34, 2:45, 2:60-61, 2:64, 6:29, 6:44-45, 6:48, 9:5-6, 9:8-9, 9:34, 10:11, 11:24. In each of these references, the word "dynamic" is tacked on to the name of a component without any context being provided for *what* makes that structure dynamic.

The prosecution history of the '004 Patent provides a little more context, even if that context is lacking from the patent itself. There, although not explicitly discussing the term "dynamic security policy," the applicant distinguished a "dynamic routing policy" because the applicant's invention "modifies the access provided to a specific user based on considerations other than his/her identity." Ex. D, Response to Office Action of Mar. 13, 2012, at 14. It noted that the then-pending claims required "modifying static authentication procedures within a network based on a dynamic rule set" and described this as a "type of dynamic modification of authentication procedures." *Id.* at 10. Nonetheless, that portion of the file wrapper does not resolve the issue of determining what is dynamic about the "rule set" referenced by the applicant, or the "security policy" claimed in the patents; it just implies that the system in some way updates these security policies on its own.

Defendant's expert volunteers several possible definitions of the word "dynamic." He suggests that "policies require frequent updates to remain vigilant against novel attacks" and that these updated policies are therefore "dynamic." Cole Decl. ¶ 45. He also suggests that the policies "necessarily update to remain vigilant," suggesting policies are dynamic when they update themselves. *Id.* ¶ 46. He also suggests that a database must be "dynamic to address any changes in each device's compliance with security policies," suggesting that a policy is "dynamic" when it is tied to,

e.g., device compliance. *Id.* He cites the prosecution history's reference to a "dynamic rule set." *Id.* He further argues that a policy is dynamic when it "allows devices to have their network access changed by the DSDPD if they become compliant with the security policy." *Id.* ¶ 57. He finally argues that these "categories" of security policies are not "mutually exclusive," but ignores that each proposed definition of "dynamic" differs in scope and changes what does and does not infringe the patent.

If a policy must be "dynamic" in that it is updated from the outside, the patent has a certain scope; if those updates must be "frequent," it has a different, and indiscernible, scope; if it must be "dynamic" in that it updates itself in response to changing circumstances, it has another scope; again if it must do so both in response to changing circumstances *and* frequently, the scope is similarly indiscernible; and if it must be "dynamic" in that it takes different actions based on different or changing circumstances, it has yet another scope. A competitor may be convinced that the security policies of their system are not "dynamic" because a system administrator has to sit down and manually modify the policy themselves. And yet, Defendant's Dr. Cole could apparently disagree if, *e.g.*, this administer makes "frequent" enough updates to "remain vigilant" to emerging threats. Or, he could disagree based upon the complexity of the policies themselves, arguing that they can "respond" to these threats on its own. In that way, whether a policy is "dynamic" becomes a "purely subjective" matter without "sufficient guidance … in the written description" or elsewhere to discern an objective standard. *Interval Licensing*, 766 F.3d at 1371. Thus, "[i]t would not be clear to a POSITA what makes a 'security policy' 'dynamic,' or, conversely, what type of 'security policy' would not be 'dynamic.'" Shamos Decl. ¶ 56. For these reasons, the term is indefinite.

b. "Dynamic Security Data and Policy Database" / "DSDPD" (Both)

Fortinet's Proposed Construction	Defendant's Proposed Construction
Indefinite	Plain and Ordinary Meaning

The term "Dynamic Security Data and Policy Database," a coined term by the patentee, Shamos Decl. ¶ 47, appears in several places in the claims of the '004 and '079 Patents. In claims 1 and 19 of the '079 Patent, a DSDPD is described as follows:

> … a **Dynamic Security Data & Policy Database (DSDPD)**, which DSDPD includes rules indicating network resource access provisions to be applied to a

> given device based on: (a) compliance of the given device with specific security policies; (b) security information received from said NSMS and (c) authentication information received from the authentication server …

Claim 10 of the '079 Patent includes the step of interacting with a DSDPD:

> … retrieving data from a **Dynamic Security Data & Policy Database (DSDPD)**, which DSDPD includes rules indicating network resource access provisions to be applied to a given device based on: (1) compliance of the given device with specific security policies and (2) security information said DSDPD retrieves from a network security and monitoring system (NSMS) comprising processing circuitry communicatively coupled to the network and configured to monitor access of end systems to the network via one or more access points; …

Claim 1 of the '004 Patent includes a module that interacts with a DSDPD:

> … a **Dynamic Security Data & Policy Database (DSDPD)**, which DSDPD includes rules indicating network resource access provisions to be applied to a given client device based on: (1) data received from the given client device indicating the compliance of the given client device with specific security policies and (2) security information said DSDPD retrieves from said NSMS …

Claim 10 of the '004 Patent includes the step of interacting with a DSDPD:

> … retrieving data from a **Dynamic Security Data & Policy Database (DSDPD)**, which DSDPD includes rules indicating network resource access provisions to be applied to a given client device based on: (1) data received from the given client device indicating the compliance of the given client device with specific security policies and (2) security information said DSDPD retrieves from a network security and monitoring system (NSMS), wherein said NSMS monitors a history of network resource access authorization requests …

Claim 19 of the '004 Patent includes the step of interacting with a DSDPD:

> … a functionally associated **Dynamic Security Data & Policy Database (DSDPD)**, which DSDPD includes rules indicating network resource access provisions to be applied to a given client device based on: (1) data received from the given client device indicating the compliance of the given client device with specific security policies; and (2) security information said DSDPD retrieves from a network security and monitoring system (NSMS), wherein said NSMS monitors a history of network resource access authorization requests …

The term invokes § 112 ¶ 6 because it is described entirely by its various functions. To the extent it purports to recite structure as a "database," that is not sufficiently definite, nor is it "sufficient structure for performing the function[s]" recited by the otherwise entirely functional claim. *Synchronoss Techs., Inc. v. Dropbox, Inc.*, 987 F.3d 1358, 1367 (Fed. Cir. 2021) (citing *Williamson*, 792 F.3d at 1349). Importantly, the "question is not whether a claim term recites *any* structure but whether it recites *sufficient* structure." *Egenera, Inc. v. Cisco Sys., Inc.*, 972 F.3d 1367, 1374 (Fed. Cir. 2020) (emphasis in original). Moreover, far from simply storing data, the DSDPD performs many other functions without providing corresponding structure. For example, it is described as being "dynamic,"

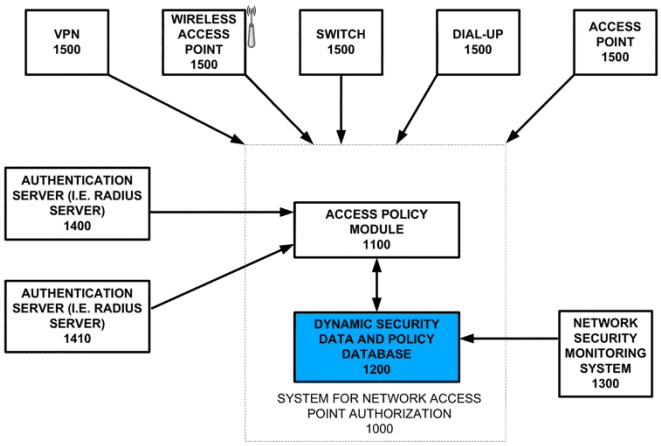
and as performing non-database functions, such as its ability to "retrieve" security information from other components in the system. In some claims, other components "receive" data from the DSDPD, suggesting that it has the ability to transmit data. *See, e.g.*, '079 Patent, Claim 1. Defendant's expert even suggests that the DSDPD "must make changes to a device's 'network access provisions'" and that it must also "change[] a device's network access based on, for example, the compliance of a given device," ascribing even more functionality to this humble database. Cole Decl. ¶ 45. The specifications further describe, in an exemplary embodiment, that the "DSDPD module may comprise a data base of security policy rules and a computational logic module functionally coupled with the data base of security policy rules and may be adapted to enforce the security policy rules," suggesting that a DSDPD may be capable of enforcing policy itself, and that it may even consist of multiple functional modules. '004 Patent, 3:40-44; '079 Patent, 3:62-66. And of course, like the term "dynamic security policy," it is unclear what is "dynamic" about the DSDPD – enough so that the term creates indefiniteness on that point alone for the same reasons.

Moreover, the slight variances in the function and data stored within the various claimed DSDPDs in the '004 and '079 Patents suggests that the function alone cannot define its structure. Shamos Decl. ¶ 54. If a DSDPD is a specific type of database that is proposed by the patentee as presenting an improvement, that improvement is, structurally, nowhere described in the patent. *Id.* Defendant's expert states that "database" connotes structure, "such as a table set up in computer memory," but the claims describe functionality that is at odds with this interpretation. Cole Decl. ¶ 51. And to the extent that "database" alone really does describe its structure, it describes the structure corresponding to only one of its many functions, leaving the rest of the DSDPD undefined and uncertain. As the Federal Circuit has observed, "[w]here there are multiple claimed functions … the patentee must disclose adequate corresponding structure to perform all of the claimed functions." *Williamson*, 792 F.3d at 1351-52. Further, the "inclusion of a limitation within a structure does not automatically render the limitation itself sufficiently structural," as "the question is not whether [the term] is utterly devoid of structure but whether the claim term recites sufficient structure to perform the claimed functions." *Egenera*, 972 F.3d at 1374. In reality, DSDPD is a long phrase used to *suggest* structure without actually connoting or denoting it for the public. If the term were replaced with

"widget," or some other nonce word, nothing else would seem to change, or that which did change is impossible to ascertain.

Putting this together, "database" in this context does not connote structure, but instead connotes one of its numerous functions: to store data. The written description fares no better at providing the structure needed. Nothing there provides guidance to assist a POSITA in determining whether a given structure is, in fact, a DSDPD. Shamos Decl. ¶ 50. This is because it is, in fact, a black box for performing its many varied functions, and is not described structurally. *Id.* ¶ 51. The term DSDPD is used, but not defined, in several places in the specification. *See* '004 Patent, 2:17-21; 2:35-40, 3:30-33, 3:40-49, 3:50-54, 11:1-8; Shamos Decl. ¶ 49. And yet – like the claim, the specification lists some of the things a DSDPD may do, but does not explain what a DSDPD is, or provide the guidance necessary to determine whether a particular database is or is not a DSDPD. Shamos Decl. ¶ 50. This compounds the uncertainty provided by the words themselves – does it refer to "dynamic security data" and "dynamic security policy," or a "dynamic database" of "security data" and "security policy"? In either event, as noted above, the term "dynamic" introduces more confusion.

In the figures in both patents, the DSDPD is shown as a black box component of the overall system, connected to the "access policy module" and the "network security monitoring system," but its constituent components, whatever they may be, are not described:



'004 Patent at FIG. 1

Finally, to the extent the many functions it performs are delineated in the claims, no algorithm is disclosed for performing these functions. The specification describes where the DSDPD sits in

relation to some other components and what functions it performs, but leaves out both its structural definition and a clear description of how it performs these functions. Courts "require that the specification disclose an algorithm for performing the claimed function," and the specification includes no such algorithm or description of how the DSDPD carries out the many tasks it is burdened with. *Williamson*, 792 F.3d at 1352. It seems the DSDPD must at least store data, send and transmit messages, enforce policy, and generally be in some way "dynamic," but the specification does not clarify how it does these things. Overall, a POSITA given a database is left unsure of whether or not that database is a "Dynamic Security Data and Policy Database," and this renders the claim indefinite.

c. "Dynamic Security Authentication Service Server" / "DSASS" ('079)

Fortinet's Proposed Construction	Defendant's Proposed Construction
Indefinite	Plain and Ordinary Meaning

The term "Dynamic Security Authentication Service Server," or DSASS, is another coined term by the patentee, Shamos Decl. ¶ 59, and appears in two of the independent claims of the '079 Patent. Specifically, Claims 1 and 18 recite a system comprising a DSASS, in turn comprising processing circuitry coupled to various other components on the network, plus the DSDPD referenced above and an "access policy module," described as follows:

> … a **Dynamic Security Authentication Service Server** (DSASS) comprising processing circuitry communicatively coupled to the network, the one or more access points, said NSMS and an authentication server external to said DSASS, said DSASS including: …

The specification does not define or even reference the DSASS. The '079 Patent is a continuation of the application that issued into the '004 Patent, and so it contains a substantively identical specification. The term "DSASS" was coined by the applicant and added to the '079 Patent claims during prosecution, in an amendment, with no explanation except to state that no new matter had been added. *See* Ex. E, Response to Office Action of June 20, 2014; Shamos Decl. ¶ 60. In the specification, the most similar-seeming component described is the "Dynamic Security Authentication Service *Proxy* server," or DSASP. Though it carries out similar functions, the DSASP itself appears in other claims – claims 7 and 20 – suggesting that, under the doctrine of claim differentiation, there must be some difference between the two. Shamos Decl. ¶ 61. These dependent claims recite that the DSAS**S** *is* a DSAS**P**, suggesting that a DSAS**P** is itself a specific type of DSAS**S**, compounding the confusion.

The difference, then, is unclear. *Id.* Moreover, the recitation that this DSASS is "dynamic" introduces the same issues as with respect to the above DSDPD and "dynamic security policy," and additionally leaves unclear whether it refers to a "dynamic security authentication service," the use of "dynamic security authentication," or simply a "dynamic … server." Shamos Decl. ¶ 62, 63. This alone is enough to independently render the claim indefinite. *Id.*

Like the DSDPD, the DSASS is described almost entirely by the function it carries out, and without reciting sufficient structure. This invokes § 112 ¶ 6. As noted above, "the question is not whether [the term] is utterly devoid of structure but whether the claim term recites sufficient structure to perform the claimed functions." *Egenera*, 972 F.3d at 1374. As it relates to structure, the term recites that it is a "[s]erver" comprised of "processing circuitry" which actually carries out the functions of the DSASS. It must also be distinct from the "authentication server" referenced elsewhere in the claims, and it is somehow broader than the DSASP referenced in claims 7 and 20. Shamos Decl. ¶ 63. However, this generic processing circuitry "amount[s] to nothing more than a general-purpose computer" programmed (in unspecified ways) to carry out these steps. *HTC Corp. v. IPCom GmbH & Co., KG*, 667 F.3d 1270, 1280 (Fed. Cir. 2012). The patent itself explains that its invention may be implemented using "a general-purpose computer selectively activated or reconfigured by a computer program stored in the computer." '079 Patent at 5:60-6:21. Moreover, this generic "processing circuitry" carries out varied functions like a general purpose computer, and is distinct from the kinds of special purpose "circuitry" that courts have found to be structural. *Cf. Qualcomm Inc. v. Intel Corp.*, 6 F.4th 1256, 1267 (Fed. Cir. 2021) (noting that claimed "power tracker" circuitry was described to "include a range of specific structural circuits"). These functions include the hosting of a "dynamic security authentication service," whatever that may be, and those of the DSDPD, itself indefinite as described above, and the recited method steps of the "access policy module."

Where the "structure amounts to nothing more than a general-purpose computer," courts have held that "the specification must disclose the algorithm that the computer performs to accomplish that function." *Qualcomm*, 6 F.4th at 1266; *accord HTC Corp.*, 667 F.3d at 1280. Far from disclosing an algorithm, the specification here does not even reference the DSASS. It does reference a DSASP, which, as discussed above, is seemingly a sub-type of DSASS. FIG. 4 even provides a flowchart that

explains the steps performed by system 1000, which is the DSASP, '079 Patent at 9:4-7, and while this might provide algorithmic structure to Claims 7 and 20 that explicitly claim a DSASS that is a DSASP, it does not shed any light on the term at issue in the broader independent claims: the DSASS. The patentee chose to specifically coin the phrase 'Dynamic Security Authentication Service Server' for use in the broader claims to distinguish them from the narrower DSASP claims, and yet the specification describes only the latter. Without a clear description of the algorithm that makes generic "processing circuitry" into a DSASS such that it can achieve its described functions, the term "lacks sufficient structure and renders the claims indefinite." *Rain Computing*, 989 F.3d at 1008.

3. U.S. Patent No. 10,530,764

a. "corporate device"

Fortinet's Proposed Construction	Defendant's Proposed Construction
Indefinite	Plain and Ordinary Meaning

Claim 1 of the '764 Patent recites, in relevant part, a processing device configured to carry out a method of authenticating devices as they connect to a network, including a step to:

> … validate a client certificate corresponding to the endpoint device to authenticate the endpoint device as a **corporate device**, wherein to validate the client certificate, the processing device to: …

The claim's recitation of the term "corporate device" renders it indefinite because it is fatally ambiguous. It is not a term of art in the field, and the patent does not provide a POSITA with any guidance on what kind of device is "corporate." Shamos Decl. ¶ 64. Without guidance on *what* must be "corporate" about the device being authenticated, one is left without "an objective standard by which to define the scope of [the patent]." *Interval Licensing*, 766 F.3d at 1369. To the extent "corporate" has ordinary meaning when used to relate something to a corporation, even Defendant's expert, Dr. Cole, makes no attempt to argue that this would make sense in the context of the '764 Patent, as it discloses nothing about corporate or organizational structure. He instead argues that the term "corporate device" means *any device* that has been successfully authenticated in accordance with the rest of the method. Cole Decl. ¶ 70. This proposal would effectively read out the phrase "as a corporate device" from the claim, requiring only the validation of the certificate, and is far from the plain and ordinary meaning of the term. If the patentee had intended this meaning, they could have

simply left that phrase out, as it is never referred to in the rest of the claims.

During prosecution, the applicant successfully refuted that the term simply means any authenticated device, distinguishing a reference by arguing that it "does not teach the authentication of an endpoint device as a corporate device," even though the reference did seem to address the validation of a certificate for authentication. Ex. F, Response to Office Action of Nov. 2, 2018, at 10. In response, the Examiner cited an additional passage from the reference, disclosing a "secure enterprise VPN gateway," and an "enterprise network" as teaching this element. Ex. F, Office Action of Feb. 27, 2019, at 3. While this illustrates that the term was not meant by the patentee to be a meaningless placeholder for any authenticated device, it is entirely unhelpful in determining what a "corporate" device *is*, except that it is similar to a device on an "enterprise" network.

The specification is also unhelpful. At points, it distinguishes between a "corporate endpoint" and "rogue device," '764 Patent at 1:51-62, and between "corporate devices" and "unauthorized devices," *Id.* at 2:60-63, without explaining the significance of these distinctions. It also largely restates the claim language, which is similarly unhelpful. *See id.* at 5:29-32, 7:12-18. All of this leaves a POSITA uncertain of what must be "corporate" about a device for it to be a "corporate device." Is its user a corporation? An employee of a corporation? Is the device owned by a corporation? Is the device connecting to a network operated by a corporation? What about other kinds of business entities? *See* Shamos Decl. ¶ 68. An indefiniteness problem arises when a claim "might mean several different things" and "no informed and confident choice is available among the contending definitions." *Interval Licensing*, 766 F.3d at 1371 (citing *Nautilus*, 572 U.S. at 911 & n.8). In this respect, the term "corporate" is similar to a term of degree, in that without specifying *what* must be "corporate" about a device, we are left with a "purely subjective" claim term, without "sufficient guidance … in the written description." *Id.* The term is therefore indefinite.

4. U.S. Patent No. 10,652,116

a. "determine a device type classification"

Fortinet's Proposed Construction	Defendant's Proposed Construction
Indefinite	Plain and Ordinary Meaning

Claim 11 of the '116 Patent recites a system having a processing device, where the processing

device carries out a method including the step to:

> … periodically **determine a device type classification** for the device based on the data associated with device; and …

This language creates multiple definiteness issues. First, it leaves unclear what a "device type classification" is, how it differs from a "device classification," and what, concretely, is and is not a device type. Second, the use of a generic "processing device" to "determine" this classification "based on" data invokes § 112(f), or means-plus-function rules, without corresponding structure in the specification. Apart from a description of the data to be used as input, there is no algorithm or method disclosed for actually making the classification itself.

First, the term's recitation of a "device type classification" creates uncertainty in what, exactly, must be determined by the processor. The doctrine of claim differentiation is "the common sense notion that different words or phrases used in separate claims are presumed to indicate that the claims have different meanings and scope." *Karlin Tech., Inc. v. Surgical Dynamics, Inc.*, 177 F.3d 968, 971-72 (Fed. Cir. 1999). Here, Claim 1 recites the determination of a "device classification," while Claim 11 recites the determination of a "device type classification," strongly suggesting that the term "type" here is, in some way, narrowing. The intrinsic evidence backs this up, with one paragraph even using both terms in the same paragraph, explaining that a classification determiner may "determine a classification of a device," and may "*further* store a device type classification of the device," although without clearly delineating the difference. '116 Patent, 8:44-53; Shamos Decl. ¶ 71.

Defendant's expert suggests that the word "type" here means that the devices may be classified into different groups "based on types of devices," and notes that the specification does give examples of "groups" based upon device type, such as "devices that have a particular operating system," "medical devices," and "operational technology devices." Cole Decl. ¶ 78 (citing '116 Patent at 3:59-4:13). However, the patent leaves unclear what distinguishes a categorization into groups that *are* based upon "device type" from groups that are not. As Dr. Shamos notes, a "potential infringer would not be able to tell whether a proposed system would infringe claim 1 … and would or would not infringe claim 11" since there is "still no basis on which to distinguish the two." Shamos Decl. ¶ 73.

Second, even if the term "device type classification" were clear, which it is not, the claim's

recitation of pure function performed by a generic "processing device" invokes means plus function claiming, and the specification provides no guidance on an algorithm for making such a determination. While a "processing device" may connote a general purpose computer, which in some claims may provide structure, this is true only where there is "enough to transform the disclosure of a general-purpose microprocessor into the disclosure of sufficient structure." *Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech.*, 521 F.3d 1328, 1335 (Fed. Cir. 2008). Here, the patent claims pure function – "determining a device type classification" – without reciting "any specific algorithm" for performing this function. *Id.* at 1331. Without such an algorithm, or any "step-by-step process for performing the claimed functions," the claim lacks the structure necessary for performing the claimed method. *Id.* at 1332. This "algorithm may be expressed as a mathematical formula, in prose, or as a flow chart, or in any other manner that provides sufficient structure," but here is entirely lacking from both the claims (triggering § 112(f)), and the specification (rendering the claim indefinite). *Williamson*, 792 F.3d at 1352.

The specification provides no algorithmic structure, and simply restates the function of the claim: performing classification "based on" certain data. The Federal Circuit has found indefinite claims under § 112(f) which recite a function to be performed "based upon" a certain type of data, but do not recite *how* that data is used. In *Traxcell Technologies, LLC v. Sprint Communications Co. LP*, the court invalidated a claim reciting a step to "suggest" certain actions "based upon" specified types of "performance data." 15 F.4th 1121, 1133 (Fed. Cir. 2021). The court noted that the patentee "had not explained how that structure in the specification *actually* provides" these suggestions, and that the specification instead "offered speculation about how [the data] *might* be used," which provides "nothing more than a restatement of the function." *Id.* at 1134 (emphasis in original). Here too, nothing in the specification provides any algorithm or steps for *how* to use this data to perform a classification, only steps for *what* to use it for: to make the classification. Moreover, it provides no algorithm for determining *any* device classification, let alone the narrower "device type classification," itself a term that is far from clear on its own. Thus, without any attempt at algorithmic structure in the patent, it is indefinite.

5. U.S. Patent No. 10,652,278

a. "standard based compliance rule"

Fortinet's Proposed Construction	Defendant's Proposed Construction
Indefinite	Plain and Ordinary Meaning

Claim 1 of the '278 Patent recites, in relevant part, a method relating to compliance monitoring of devices on a network, comprising the step of:

> … accessing a compliance rule based on the classification of the device, wherein the compliance rule is a **standard based compliance rule**; …

This claim's recitation that the compliance rules must be "standard based" presents multiple issues to one attempting to ascertain the scope of the claim. First, the word "standard" has competing meanings, and apparently references the whims of outside standards-setting organizations or even de-facto standards. Second, the fact that these rules must only be "standard *based*" implies that the already-vague word "standard" is being applied using a term of degree, with no clear guidance provided as to how related a compliance rule must be to a standard in order to trigger infringement. Together, these issues render the term indefinite.

First, the term "standard" is amenable to multiple meanings. It could refer to the language in which the "compliance rules" are written – the specification references "SCAP," which is "a set of open standard XML based languages for writing configuration benchmarks for computing devices." Shamos Decl. ¶ 76; '278 Patent, 2:21-24. Under that reading, a compliance rule must be written in SCAP or another standard language to be "standard based," although this still leaves open the question about what a standard language is apart from the example of SCAP. Alternatively, it could refer to a rule which implements a standard. In either case, as Dr. Shamos explains, the "process by which a set of rules becomes a 'standard' is undefined – some 'standards' simply become de facto standards through common acceptance, although it is not clear exactly when this occurs, and there is no definitive way of telling what is and what is not a standard." Shamos Decl. ¶ 77.

Defendant's expert, Dr. Cole, appears to gravitate towards this latter interpretation, arguing that a rule is standards based "if a standard describes that compliance rule," and that the claim "encompasses any compliance rule based on a standard" with no limitations. He then somehow asserts that the term needs no construction and should be afforded its plain and ordinary meaning. Cole Decl.

¶ 31. This would go against the specification, which only describes SCAP as a "language for writing configuration benchmarks," not actually a set of compliance rules, and in any event fails to answer the even more difficult question of defining a standard. '278 Patent, 2:21-24. Under either interpretation, without "an objective standard" for defining "standard," the claim scope is far from reasonably certain to a POSITA. *Interval Licensing*, 766 F.3d at 1369.

Moreover, even if it were clear what is or is not a standard, and who may define them, which it is not, the use of the term opens up difficult infringement issues as standards can be changed, and that which was an unstandardized industry practice can suddenly become an accepted standard at any time. This means that a standards body (or, under a broader read of "standard," anyone) can adjust the scope of this patent at any point, without the consent or knowledge of those now practicing the patent. Shamos Decl. ¶ 81. It is an issue not dissimilar from one explored by the Federal Circuit in *Medicines Co. v. Mylan, Inc.*, where it held a patent claim indefinite because "proof of infringement would necessitate forward-looking assessments," as the outcome of tests on future batches of a pharmaceutical product could render the previous batches suddenly infringing. 853 F.3d 1296, 1303 (Fed. Cir. 2017). Furthermore, given the existence of "closed standards," ones that are "proprietary or secret" or that are "not endorsed by a standards body," it is even possible that such a standard could arise and those practicing the rest of the patent would have no way of knowing about it. Shamos Decl. ¶ 78. Defendant's expert responds that the patent is unlimited in scope on this point, that it "is not limited to any particular standard or any particular time frame but rather encompasses any compliance rule based on a standard." Cole Decl. ¶ 92. Apart from the inherent circularity of arguing that a compliance rule is "standards based" when it is "based on a standard," Dr. Cole appears to submit that the scope of this claim changes due to the future and undisclosed actions of third parties, which should on its own render the claim indefinite.

Second, even if all of the above were clear, and a POSITA could state with certainty whether or not something was in fact a standard, they would have difficulty determining if something is "based on" that standard. Defendant's expert submits that a compliance rule is standard based "if a standard describes that compliance rule," suggesting that if any part of a standard describes the rule, the rule infringes this element. Cole Decl. ¶ 92. But he cites no support for this opinion, and makes no attempt

to distinguish alternate meanings. On the broader side, it could mean that a rule would infringe if it is written to ensure compliance with a standard that describes the desired state of a machine but does not describe the specific rule of how to determine that state. On the narrower side, it could mean that the exact rule itself must be a standard. The phrase "based," rather than, *e.g.*, "defined" or "described," suggests a level of flexibility in how closely the compliance rule must track a standard, but provides no "objective boundaries" for that flexibility, creating uncertainty and indefiniteness. *Interval Licensing*, 766 F.3d at 1371. Combined with the distinct lack of clarity in defining what is and is not a "standard," this term leaves the scope of the claim far from certain.

b. "compliance level"

Fortinet's Proposed Construction	Defendant's Proposed Construction
"quantitative score indicating the extent to which a device is in compliance with compliance rules"	Plain and Ordinary Meaning

Claim 1 of the '764 Patent recites, in relevant part, a processing device configured to carry out a method of authenticating devices as they connect to a network, including a step to:

> … determining a **compliance level** of the device based on a result of the compliance scan of the device; and …

Fortinet contends that this term refers to a "quantitative score indicating the extent to which a device is in compliance with compliance rules," while Defendant proposes that it be afforded its plain and ordinary meaning. The parties seem to disagree primarily on whether the compliance level must be a quantitative score, with Defendant's expert positing that the "compliance level" may mean "any indicator showing the extent to which a device is following compliance rules" including a "pass/no pass" indicator. To be clear, while Fortinet had originally proposed "numerical" for this element, it changed its proposal to "quantitative" to reflect that the level need not be expressed as a number – Dr. Cole's example of "high," "medium," or "low" risk, for example, is still quantitative in that it expresses a comparable quantity (or *level*) of risk. *See* Cole Decl. ¶ 84. Taking this into account, the scope of the disagreement is quite narrow, and limited to whether this "compliance level" refers to a quantity.

Importantly, "the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Phillips*, 415 F.3d at 1313. Here, <u>every</u> embodiment of or

reference to a "compliance level" in the specification is quantitative in nature, a point which Defendant's expert does not contest, except to say that they are all exemplary. Shamos Decl. ¶ 74-75; Cole Decl. ¶ 84. The specification describes a compliance level as something that is "computed," '278 Patent at 2:28-33, 3:26-32, 8:26-30, "calculated," *id.* at 3:26-32, as "percentage or number of points," *id.* at 3:26-32, 6:9-14, for example, "20%," "70%," and "80%," *id.* at 4:66-5:8, 6:24-33. Every part of the patent either explicitly states that the "compliance level" is a computed quantity, or simply treats it as such by, *e.g.*, comparing it to a threshold, *id.* at Cl. 14-15, or computing it specifically by using weights assigned to results of specific rules, *id.* at Cl. 8. As to the last point, though Dr. Cole suggests that the doctrine of claim differentiation requires that since Claim 8 recites a compliance level computed by assigning weights, Claim 1 must be broader and thus non-quantitative, he is mistaken. Cole Decl. ¶ 84. Claim 8 *is* narrower even though Claim 1 requires a quantitative level, as it just claims a *specific way* of computing this quantity, as opposed to *e.g.*, using a summation, average, maximum, or minimum of sub-scores, or any other method.

Dr. Cole suggests that these references in the specification are all exemplary. Cole Decl. ¶ 84. It is true that courts have warned against reading in exemplary embodiments from the specification, but here there is absolutely "nothing in the context to indicate that the patentee contemplated any alternative" to a quantitative compliance level. *Phillips*, 415 F.3d 1323 (quoting *Snow v. Lake Shore & M. S. Ry. Co.*, 121 U.S. 617, 630 (1887)). Moreover, this construction comports with the plain meaning of the word "level" in the claim, which implies quantity, and the fact that this "level" is "determined," whereas a qualitative or otherwise non-quantitative measurement (like a pass/fail result, or a list of test results) strips the term of meaning. If the patentee had intended that, they could have simply referenced the "results" of the compliance scan, rather than explicitly requiring one to "determine" a "level" of compliance based upon these results. Thus, a "compliance level" refers to a "quantitative score indicating the extent to which a device is in compliance with compliance rules."

V. LEVEL OF ORDINARY SKILL IN THE ART

In his latest declaration, Defendant's expert takes issue with the level of skill of Fortinet's expert, and states that he believes Dr. Shamos "does not have requisite experience to qualify as a POSITA or testify regarding the knowledge and understanding of a POSITA." Cole Decl. ¶ 21. While

Dr. Cole took no issue with Dr. Shamos's qualifications in his rebuttal to his initial report in 2021, his most recent declaration includes several such attacks. He goes so far as to seemingly mock Dr. Shamos for his age, noting that his last (and fifth) graduate degree (a Ph.D. in computer science) was received "in the 1970s," and for his publications outside of the networking field, such as on his hobby of billiards. *Id.*

Putting aside Dr. Cole's unseemly and unprofessional critique, Dr. Shamos is a well-qualified expert. As he stated in his initial report, he has "taught computer networking, wireless communication and Internet architecture since 1999" and is the "author and lecturer in a 24-hour video course on Internet Protocols." Shamos Initial Rep. (Ex. G) ¶ 10. He also teaches courses on electronic payment systems, which naturally include networking and security elements. *Id.* ¶ 9. Moreover, his extensive experience in the issues surrounding the security of electronic voting systems, which Dr. Cole dismisses as irrelevant, necessarily includes expertise in network security and network access control. He has testified before committees of the British House of Lords, the U.S. House of Representatives, and the U.S. Senate on the subject of the security of electronic voting machines. *See* Cole Rep. (Ex. B), Exhibit B (Shamos Biography), at 4-5.

It is true that the Court "confronts a ghost … not unlike the 'reasonable man' and other ghosts in the law" when considering the perspective of a person having ordinary skill in the art at the time of invention. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1566 (Fed. Cir. 1987). In claim interpretation, this "provides an objective baseline from which to begin," and is based upon the recognition that "patents are addressed to and intended to be read by others of skill in the pertinent art." *Phillips*, 415 F.3d at 1313. Dr. Shamos is a leader in his field, has a Ph.D. in computer science and decades of experience in computing, networking, and security, which allows him to provide the Court with the perspective necessary to form this objective baseline for the 10 distinct patent families at issue in this case.

VI. CONCLUSION

Based on the foregoing, the Court should adopt all of Fortinet's proposed constructions.

DATED: April 6, 2022

By: */s/ John M. Neukom*
JOHN M. NEUKOM
Attorney for Plaintiff
FORTINET, INC.

Exhibits

A. Claim Construction Declaration of Dr. Michael Shamos on Forescout Patents, Apr. 5, 2022

B. Rebuttal Declaration of Dr. Eric Cole Regarding Claim Construction of Terms in Forescout Patents, Mar. 8, 2022.

C. File History of U.S. Patent No. 6,363,489

D. File History of U.S. Patent No. 8,590,004

E. File History of U.S. Patent No. 9,027,079

F. File History of U.S. Patent No. 10,530,764

G. Claim Construction Report of Dr. Michael Shamos on Fortinet Patents, May 21, 2021